



Australian Government
Medicare Australia

Installing a location certificate with a password prompt to enable access to HPOS

User Guide for Windows Vista
(Release date: June 2009)

eBusiness service centre: 1800 700 199
Email: onlineclaiming@medicareaustralia.gov.au

www.medicareaustralia.gov.au

Table of Contents

Introduction	1
Location certificates install	1

Table of Figures

Figure 1: Index html page.....	2
Figure 2: Vista start button	3
Figure 3: Type in Run.....	4
Figure 4: Run explorer.....	5
Figure 5: Vista Windows Explorer	5

Introduction

This guide demonstrates how to install a Location Certificate protected with a password to the Microsoft crypto store, to enable access to the Medicare Australia Health Professional Online Services (HPOS).

The following instructions will work with most Microsoft Vista installs.

If you experience any problems please call eBusiness Service Centre on 1800 700 199.

Location certificates install

Important: if you do not want a prompt for a password when using location certificates to enter HPOS then please follow the User Guide *Installing a location certificate to enable access to HPOS without prompting for password at each log in (Vista)*.

To install the location certificates you will require local administration to your computer. If you do not have administration access, please discuss this with your system administrator.

Step 1

Insert the CD you have received from eCertificates, into your CD/DVD drive.

The following screen will display.

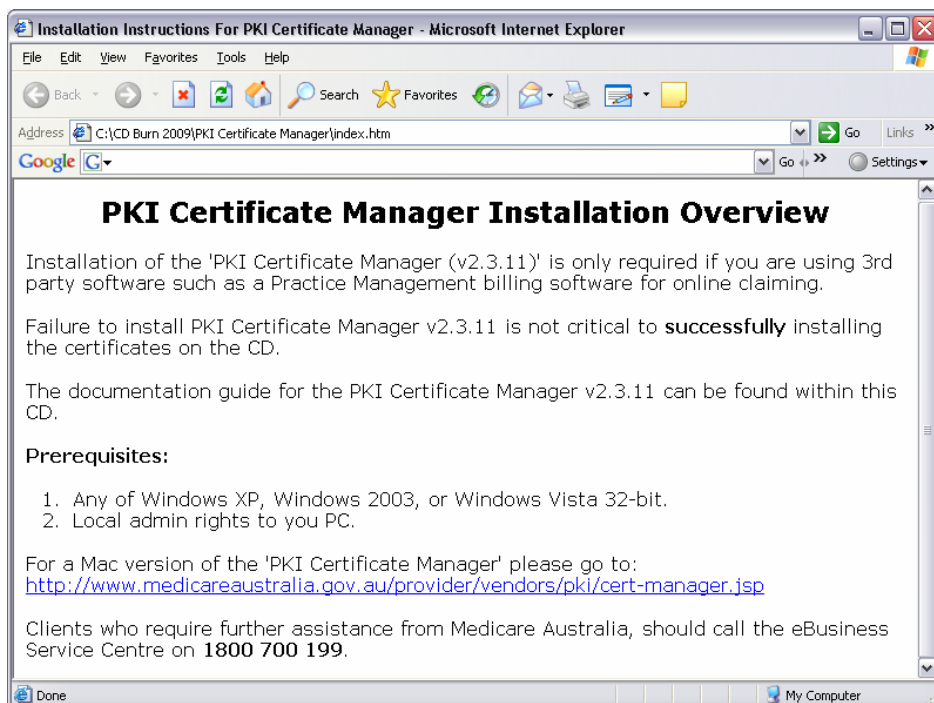


Figure 1: Index html page

Close the above screen as this relates to installations allowing online claiming.

Go to *step 2*.

Step 2

Click *Start* at the bottom left of the screen.

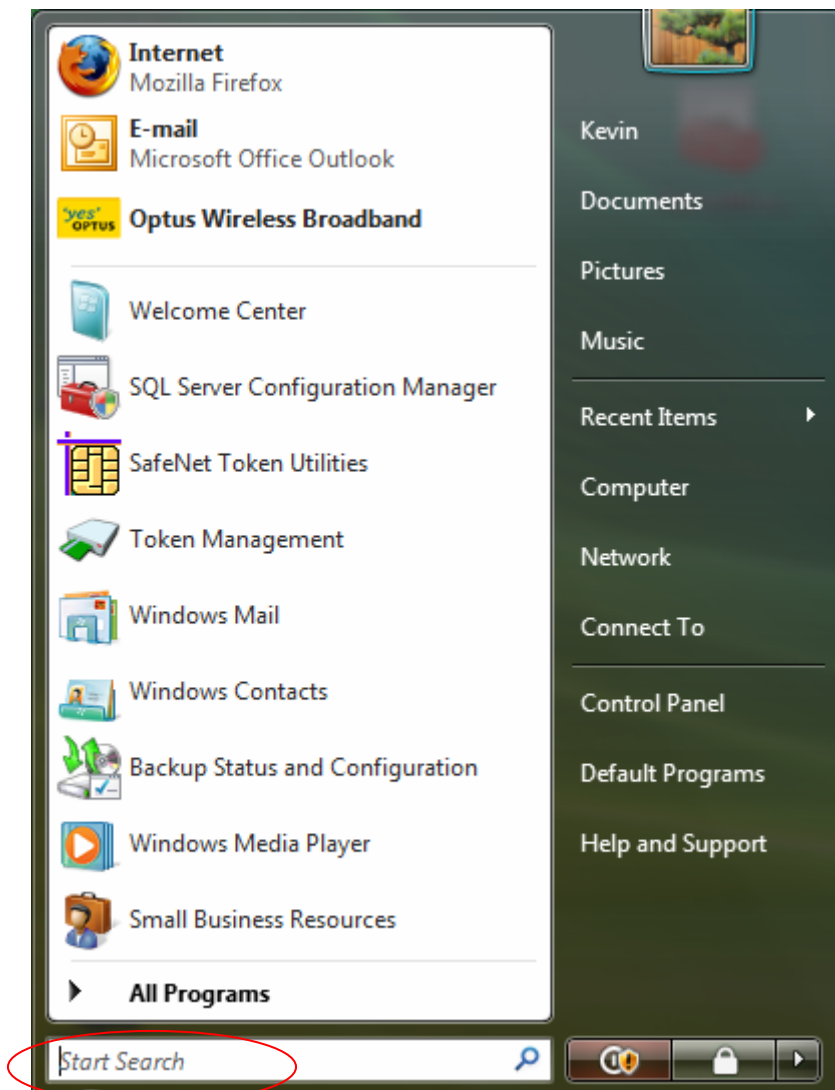


Figure 2: Vista start button

In *Start Search* type in 'run'.

Step 3

The following screen will display.

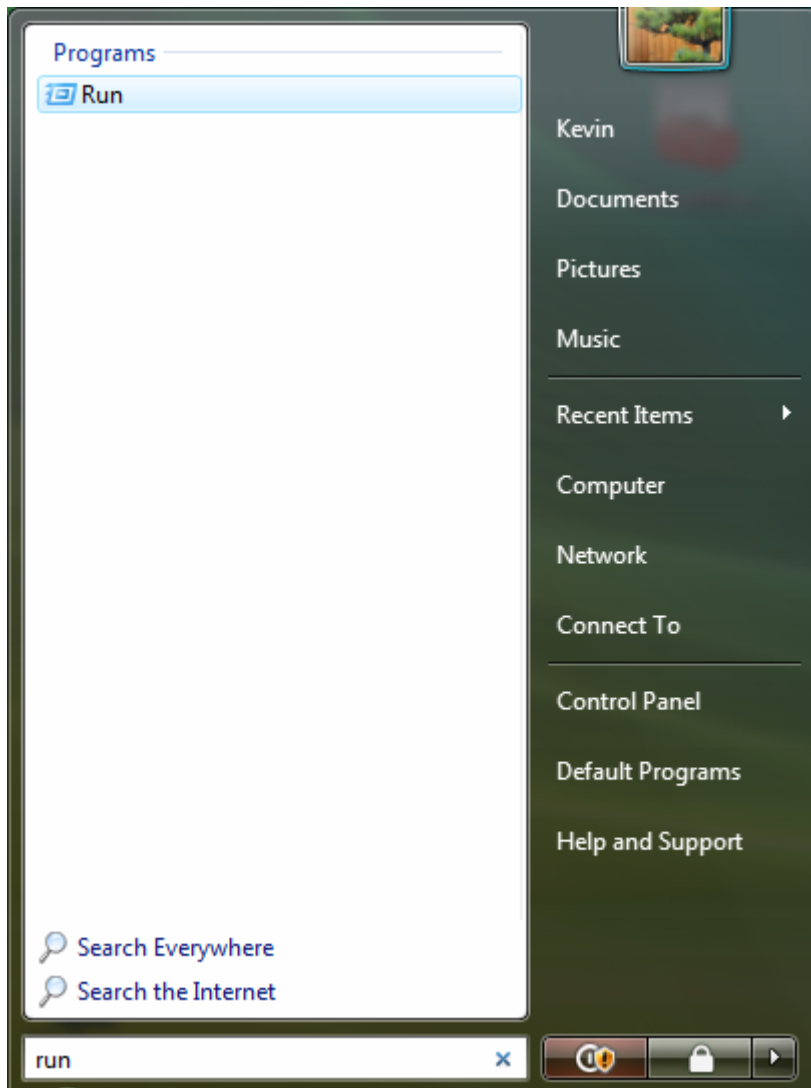


Figure 3: Type in run

Type in 'run,' and hit Enter on your keyboard to execute the program 'Run'.

Step 4

The following screen will display.

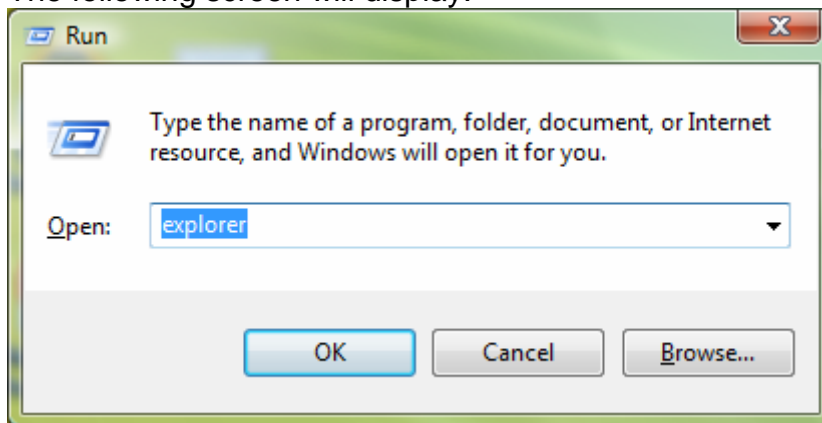


Figure 4: Run explorer

Type in 'explorer' and click OK.

The following screen will display.

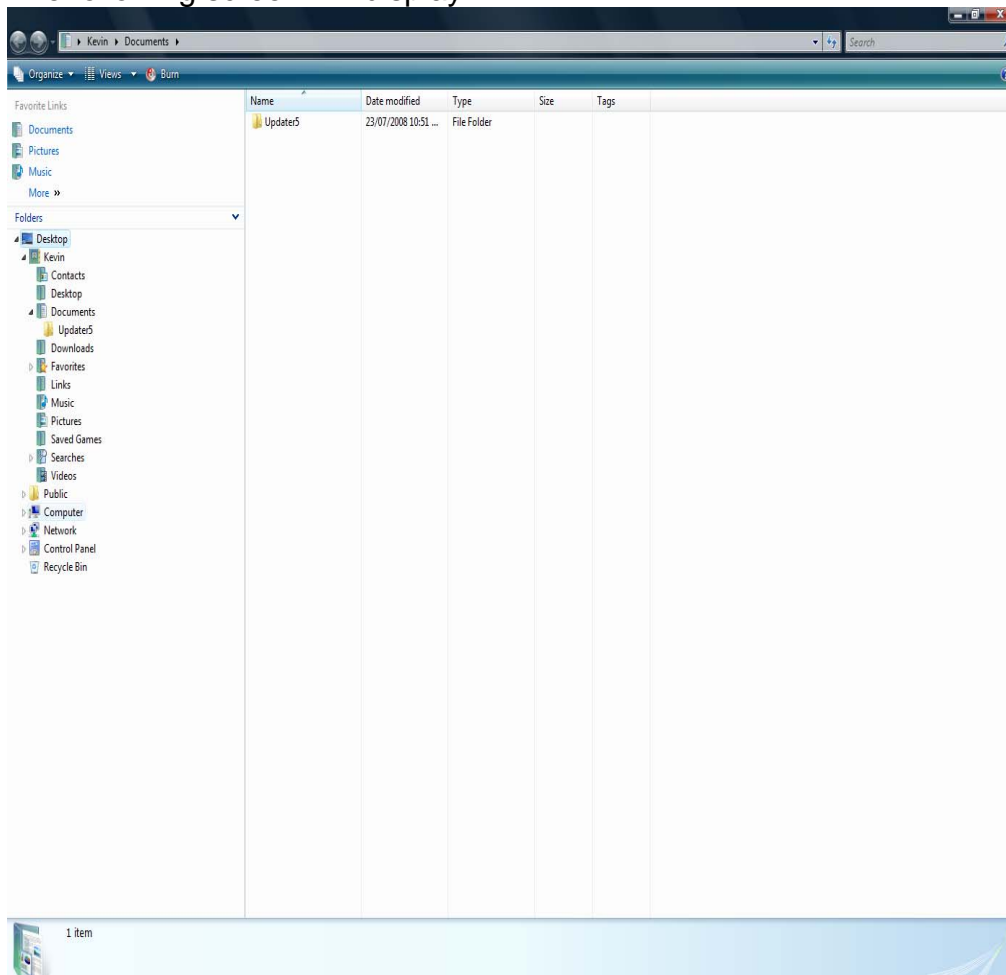


Figure 5: Vista Windows Explorer

Click on *Computer* as shown above.

Step 5

Installing location certificates with a password prompt to enable access to HPOS - Vista Version 1.0
Electronically controlled document – printed copies are Uncontrolled

The following screen will display.

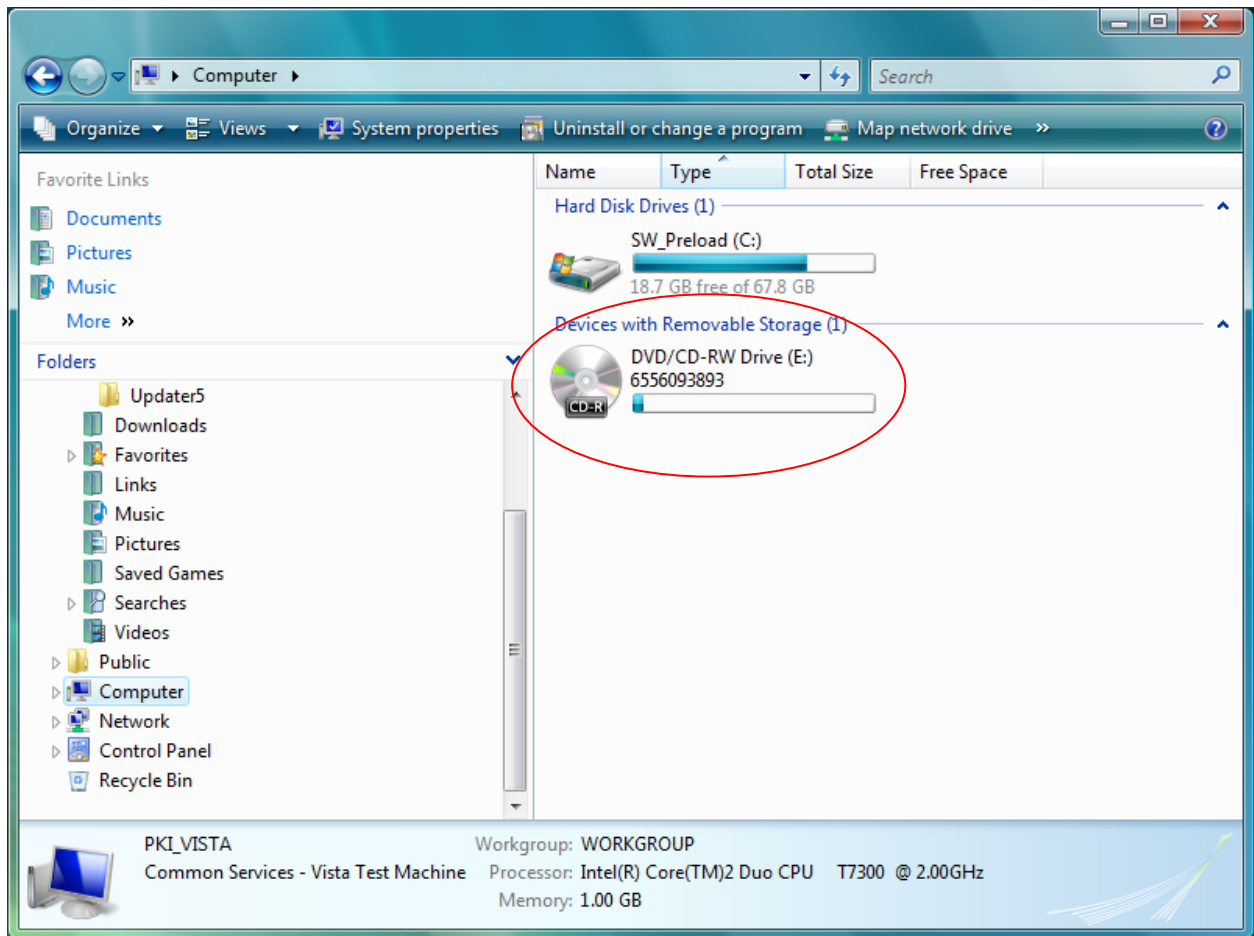


Figure 6: Vista Windows Explorer CD drive

Double click the CD/DVD drive in the right panel as shown above.

Step 6

The following screen will display.

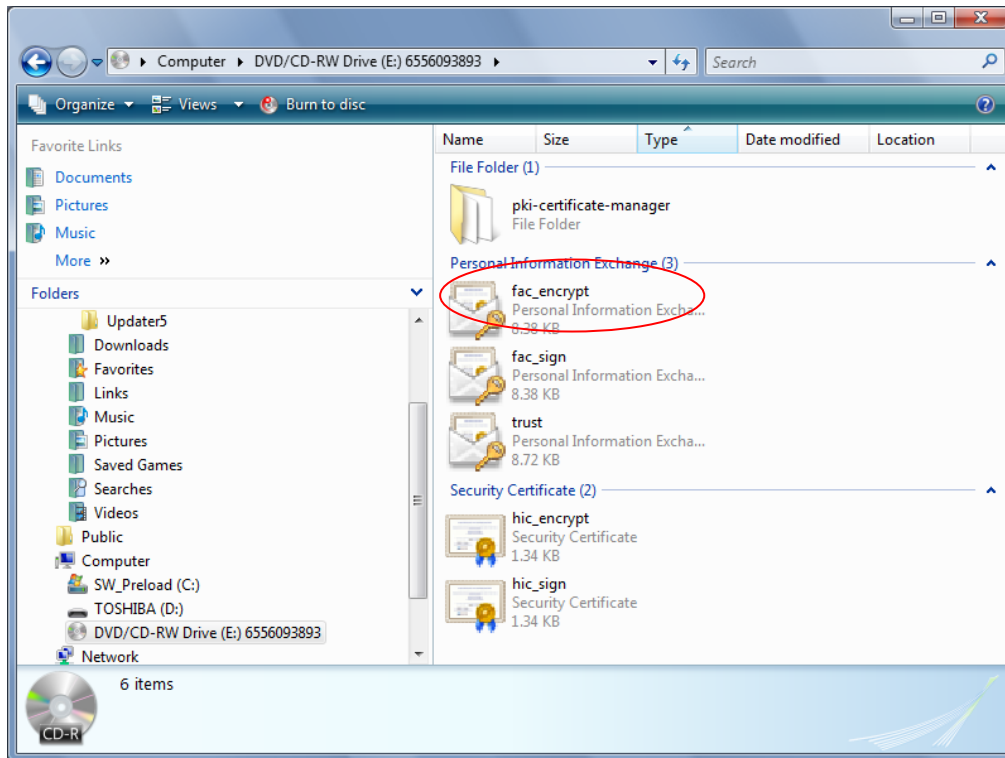


Figure 7: Windows Vista Content of CD

You will need to install two files. These are the encryption certificate and signing certificate.

- *fac_encrypt.p12*
- *fac_sign.p12*

Double click *fac_encrypt.p12* as shown in the above screen.

Step 7

A Wizard will appear.



Figure 8: Certificate Import Wizard

To continue click *Next*.

Step 8

The path of the file selected is displayed in the next screen.

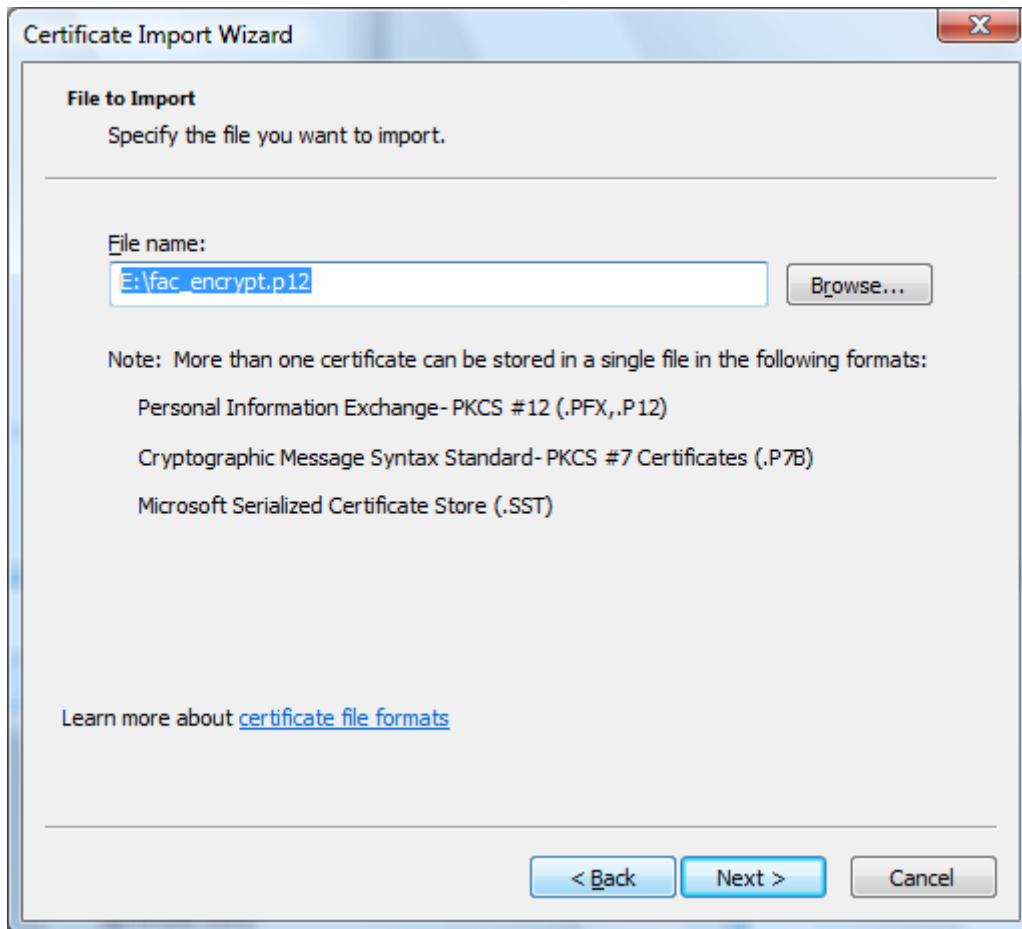


Figure 9: File to import

To continue click *Next*.

Step 9

The following screen will display.

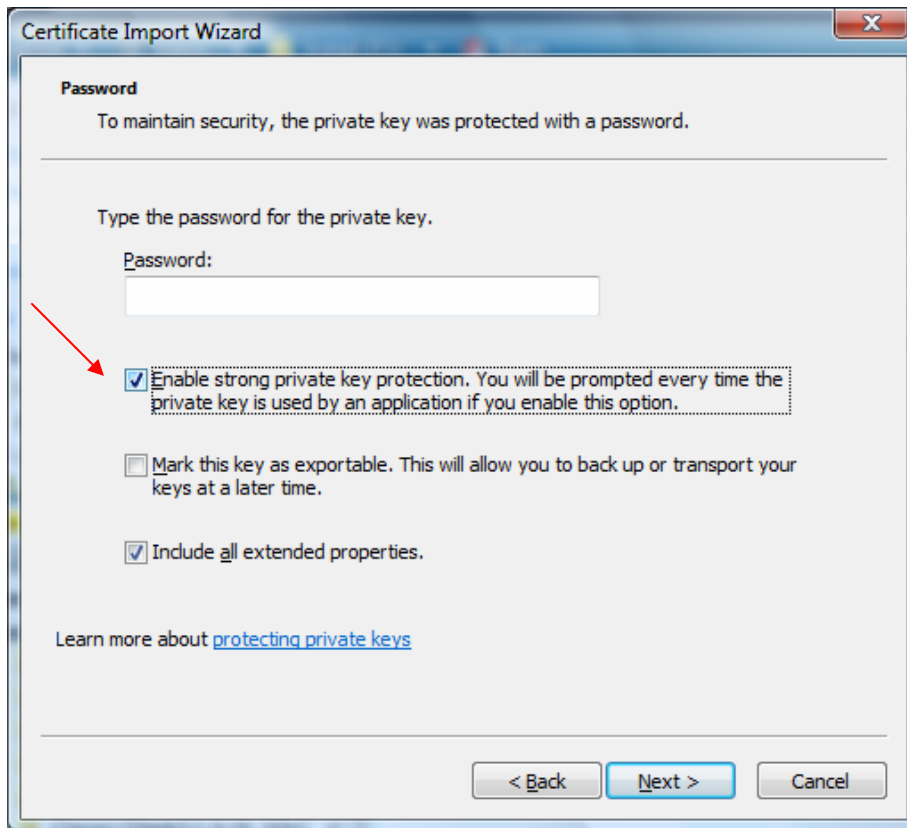


Figure 10: Windows Vista password prompt

Enter the password supplied with your new certificate, key in the (PIC) passphrase.

Tick the *Enable strong private key protection* box.

To continue click *Next*.

Step 10

The following screen will display.

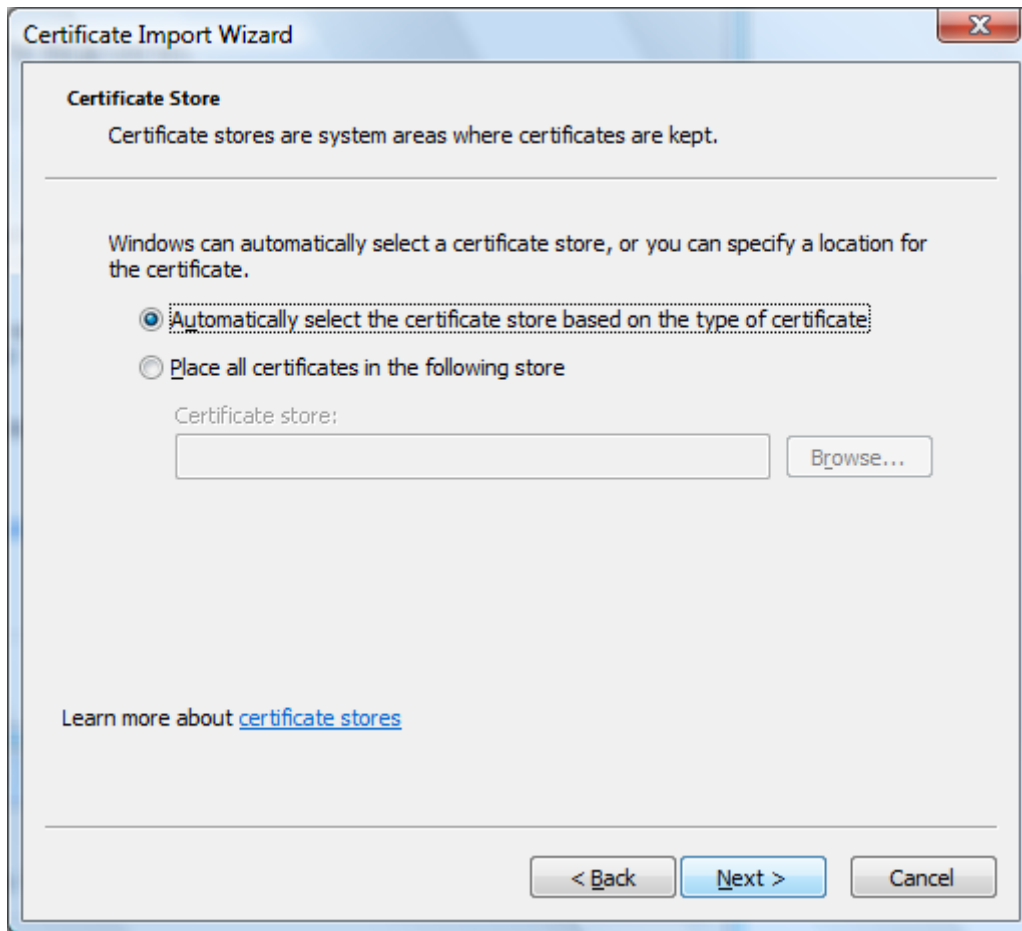


Figure 11: Certificate Import Wizard: Certificate Store

Leave the setting as they appear in *Figure 11*.

To continue click *Next*.

Step 11

The following screen will display.

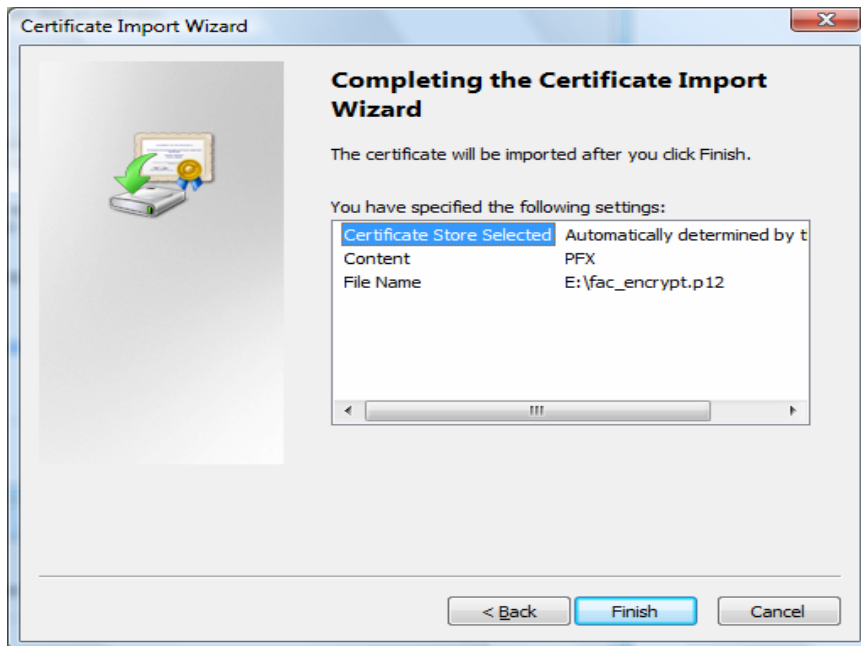


Figure 12: Certificate Import Wizard: Completing the Certificate Import Wizard

To continue click *Finish*.

Step 12

The following screen appears and will allow you to set the security level with your password.



Figure 13: Importing a new private exchange key

To continue click *Set Security Level*.

Step 13

The following screen will display.



Figure 14: Importing a new private exchange key: choose a security level

Select the 'High' radio button

To continue click *Next*.

Step 14

The following screen will display.

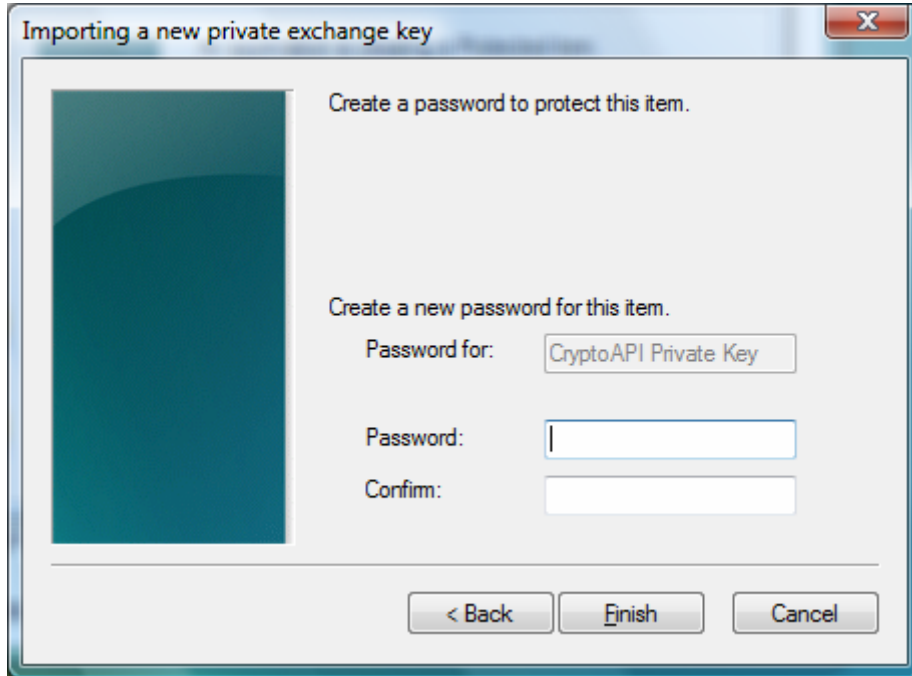


Figure 15: Importing a new private exchange key: Create password

This screen allows you to select your own password for future use. It is not the PIC pass phrase that came with the certificate.

Important. Please memorise this password as you will be prompted for this each time you use the certificate to log on to HPOS.

Choose a friendly password and key it in the password field.

Re-enter your password in the confirm field.

To continue click *Finish*.

The following screen will appear.



Figure 16: Security level set to High

To continue click *OK*.

Step 15

The following screen will appear.

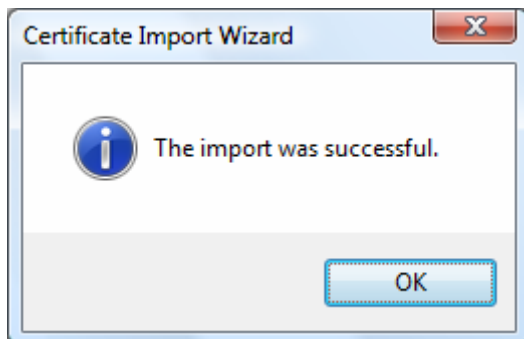


Figure 17: Certificate Import Wizard: Import successful

Click *OK* to finish.

Step 16

Repeat steps 5 - 15 to install *fac_sign.p12* signing certificate.

Important: At step 9, key the same PIC password as was keyed for *fac_encrypt.p12* (It came with the certificate). At step 14, key the same friendly password you chose with the *fac_encrypt.p12*.

You have now installed the private keys of your location certificate.

Once both files have been installed go to *step 17*.

Step 17

Installing Chain of Trust certificates for Vista

Go to the Certificates Australia website www.certificates-australia.com.au and locate the two certificates listed below under *Quick Links*.

- Root CA Certificate (under the Quick Links – Medicare Australia PKI)
- OCA Certificate (under the Quick Links – Medicare Australia PKI)

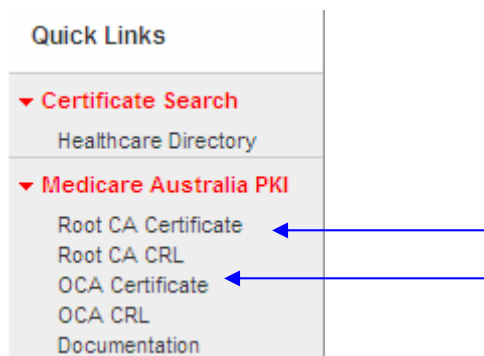


Figure 18: Verizon Website Menu links

Click the Root CA Certificate then choose *save*, to the Desktop or appropriate folder.
Click the OCA Certificate then choose *save* to the Desktop or appropriate folder.

The certificates are now ready to import into the Microsoft Management Console.

Step 18

Click on the Start button as shown in the following screenshot.

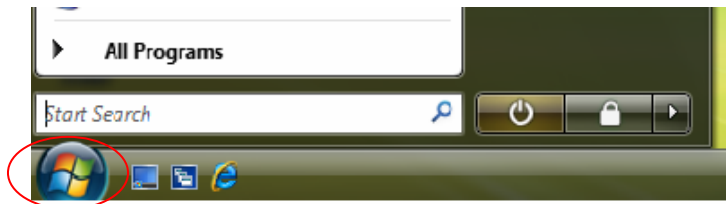


Figure 19: Vista Start button

In the search field enter 'mmc' (Microsoft Management Console) as shown in the following screenshot.

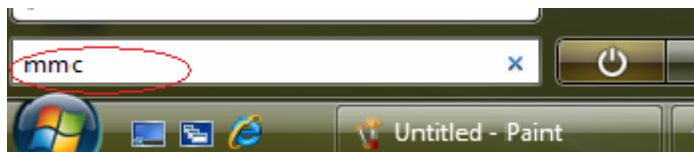


Figure 20: mmc in Start search

To continue hit *Enter* on your keyboard.

Step 19

A User Account Control dialog box will appear.

To continue click *Continue*.

The following screenshot will be displayed.

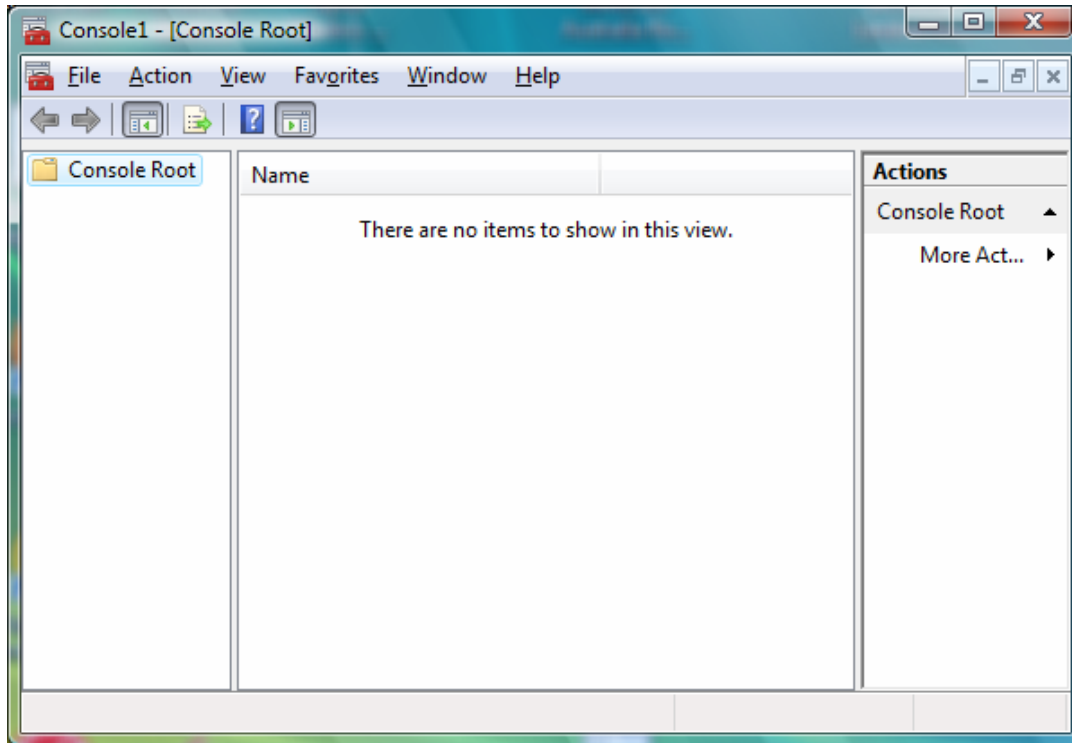


Figure 21: Console1 screen shot.

From the Console1 screen click *File* and then select *Add/Remove Snap-in* from the drop-down menu as shown in the following screen shot.

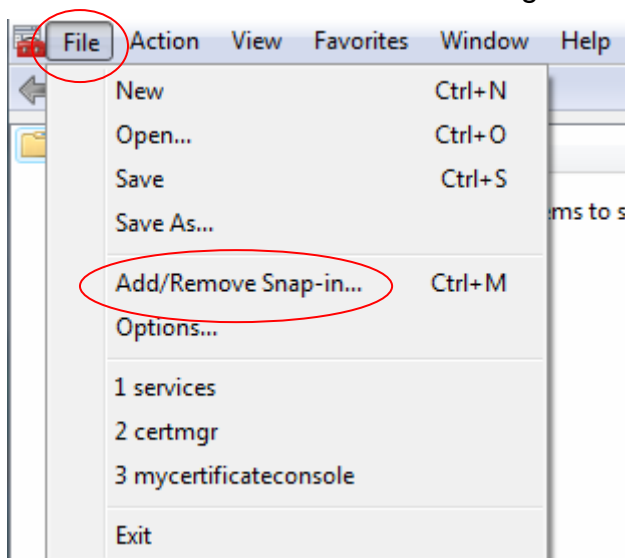


Figure 22: Console add/Remove Snap-in

Step 20

The following screen will display.

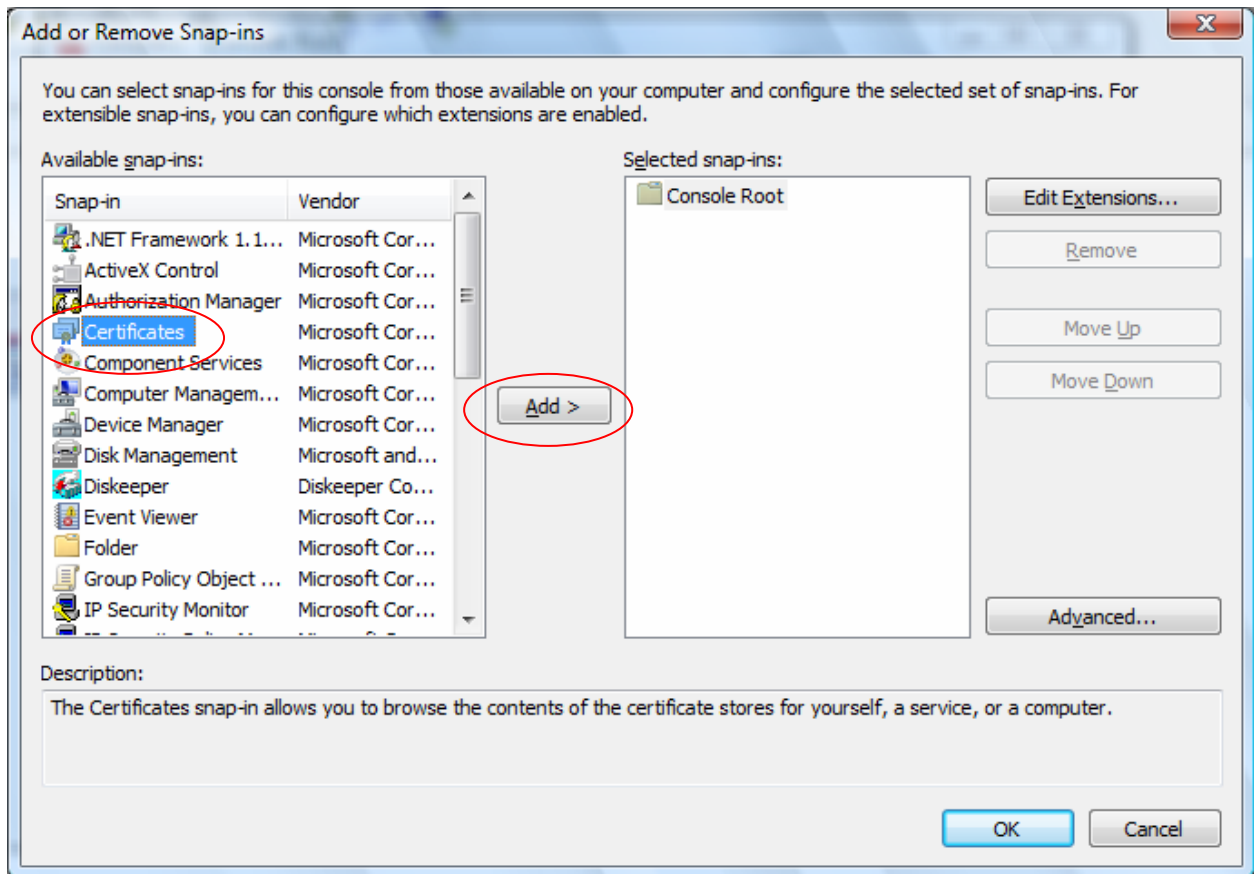


Figure 23: Add Certificates Snap-in

Select *Certificates* from the Available snap-ins list and then click the *Add* button as shown above.

Step 21

The following screen will display.

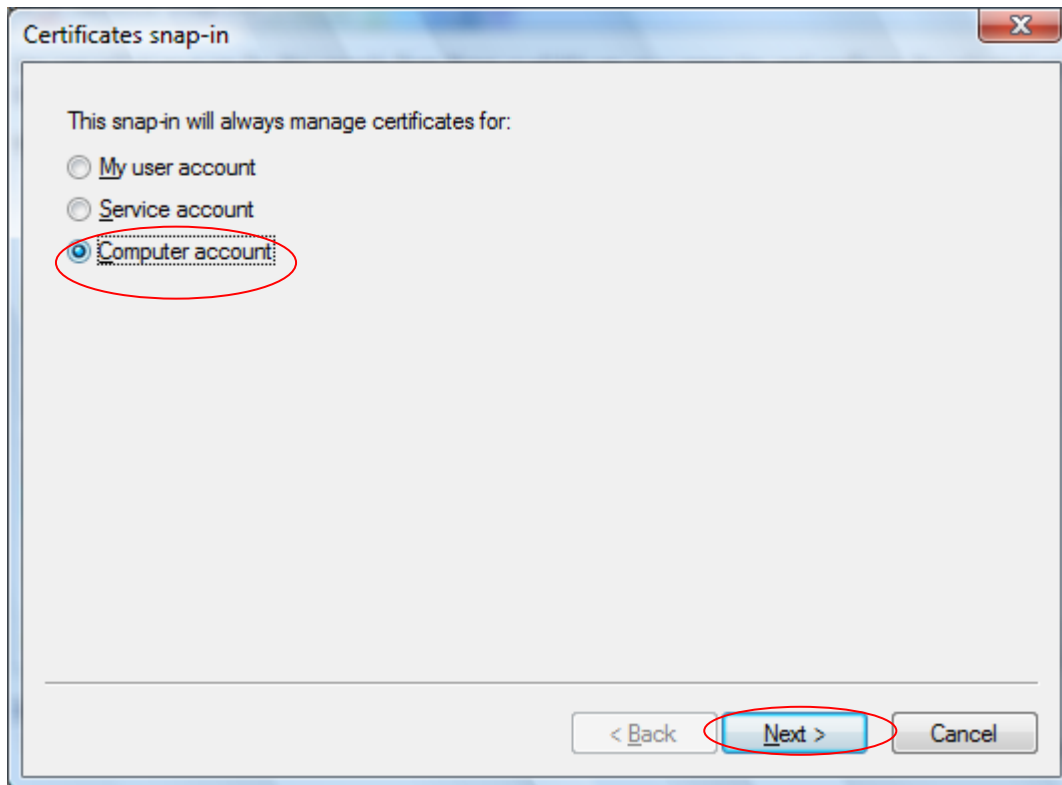


Figure 24: Select account

Choose *Computer Account*.

To continue click *Next*.

Step 22

The following screen will display

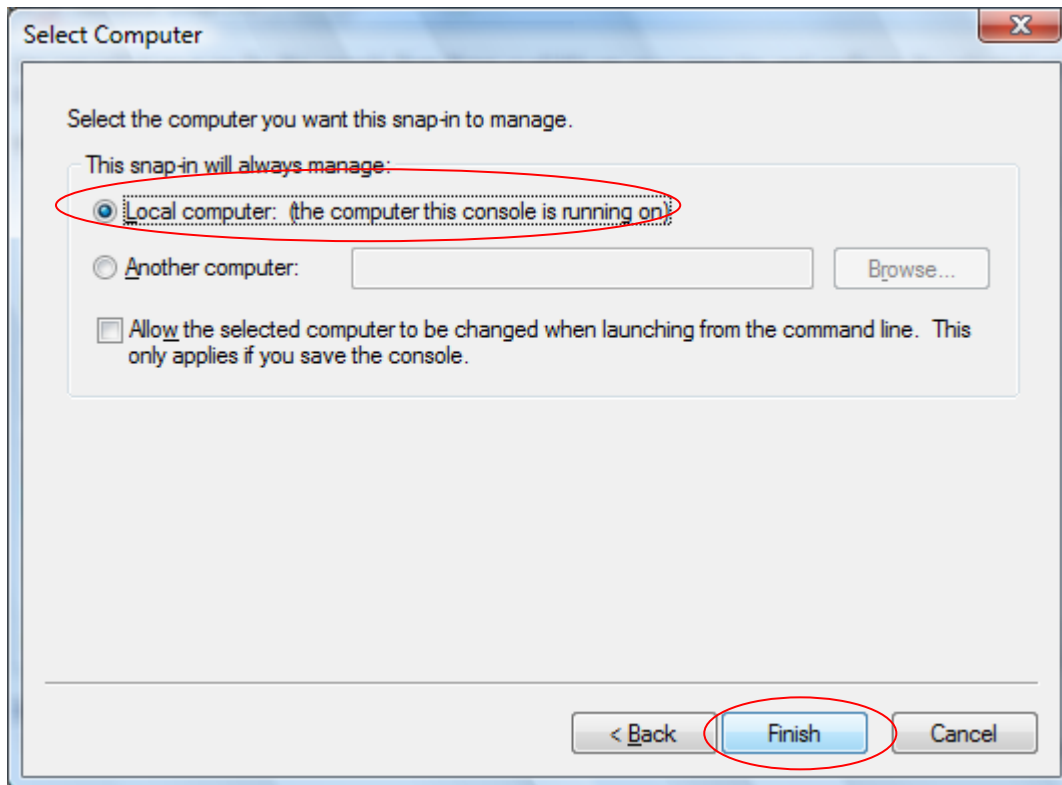


Figure 25: Select Local computer

Choose *Local Computer*.

To continue click *Finish*.

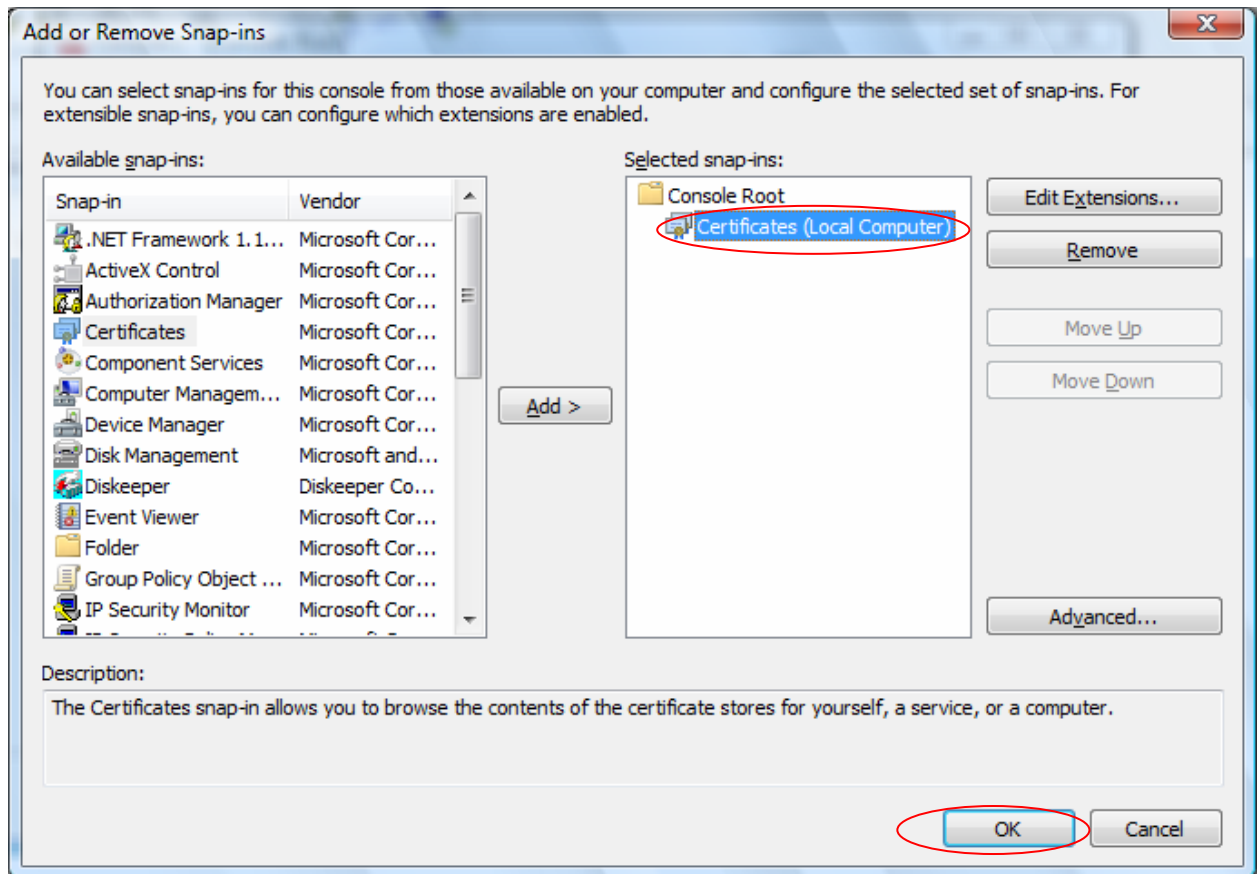
Step 23

Figure 26: Click OK

Certificates (Local Computer) will now appear as an option under the Console Root directory.

To continue click *OK*.

Step 24

The following screen will display.

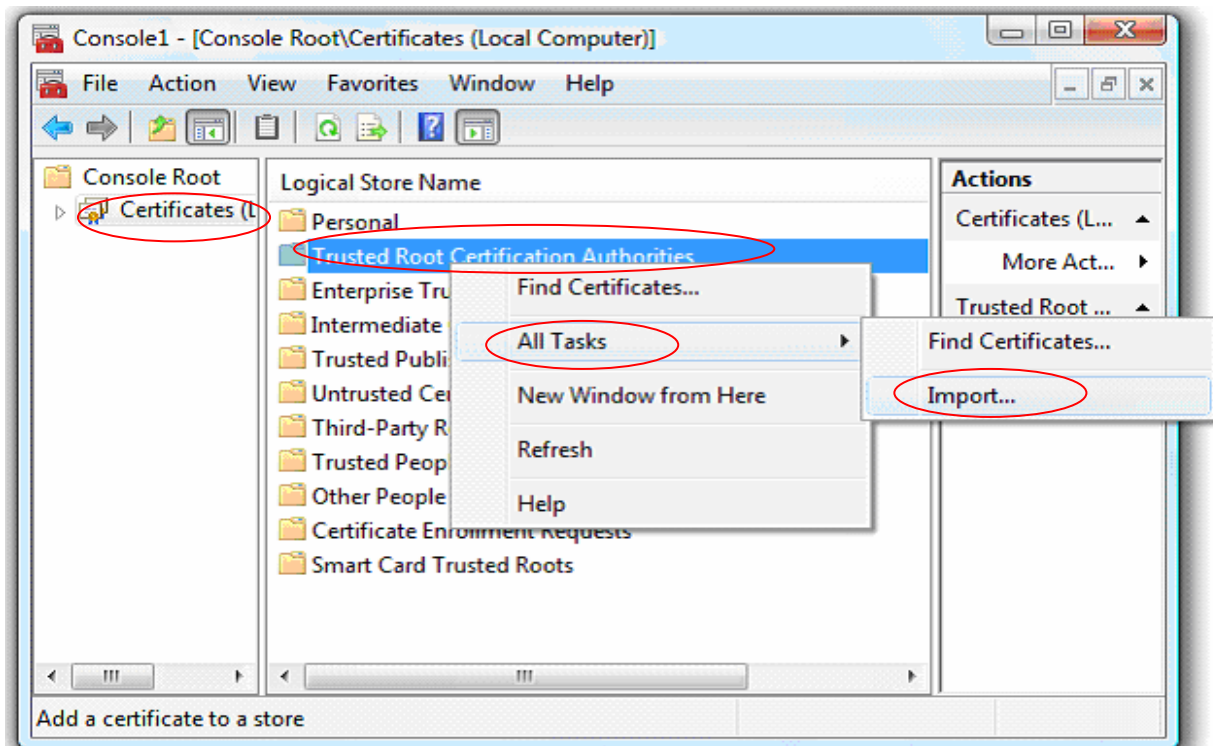


Figure 27: Select Import

Click on *Certificates (Local Computer)* and then right-click on *Trusted Root Certification Authority*.

Select *All Tasks* and then click on *Import* as shown above.

Step 25

The following screen will display.

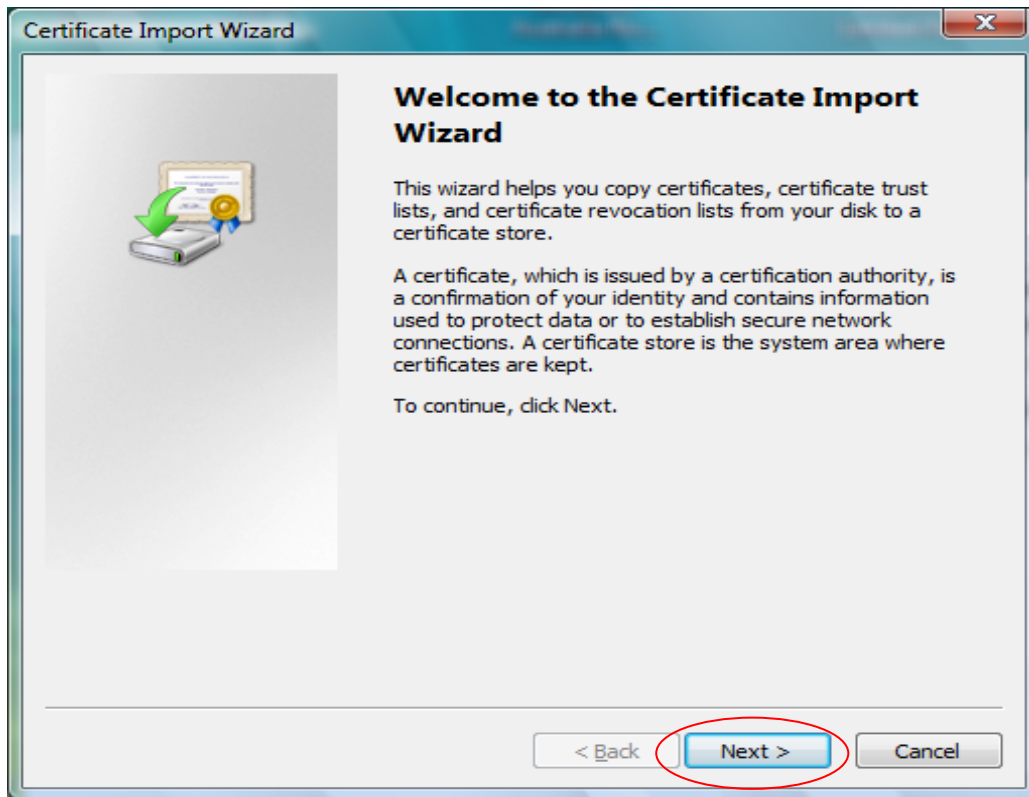


Figure 28: Click Next button.

To continue click *Next*.

Step 26

The following screen will display.

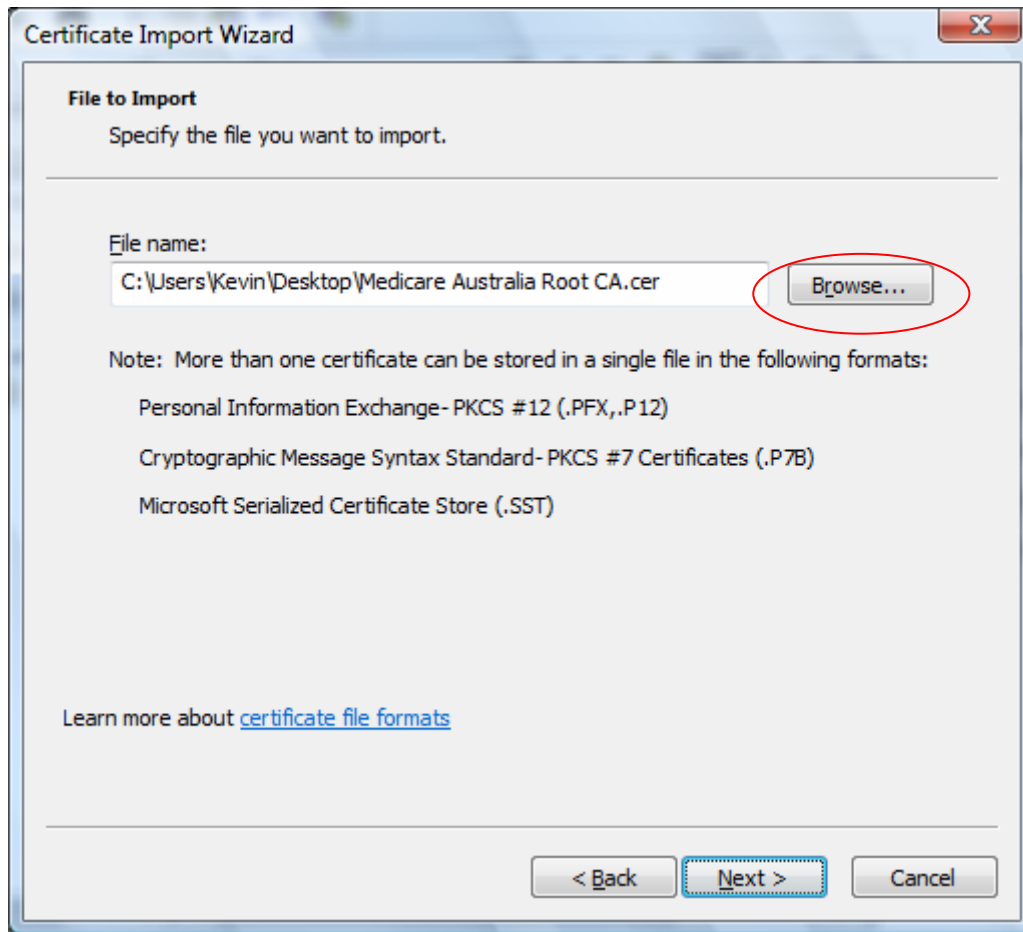


Figure 29: Select Medicare Australia Root CA.cer

Click *Browse* as shown above.

The following screen will display.

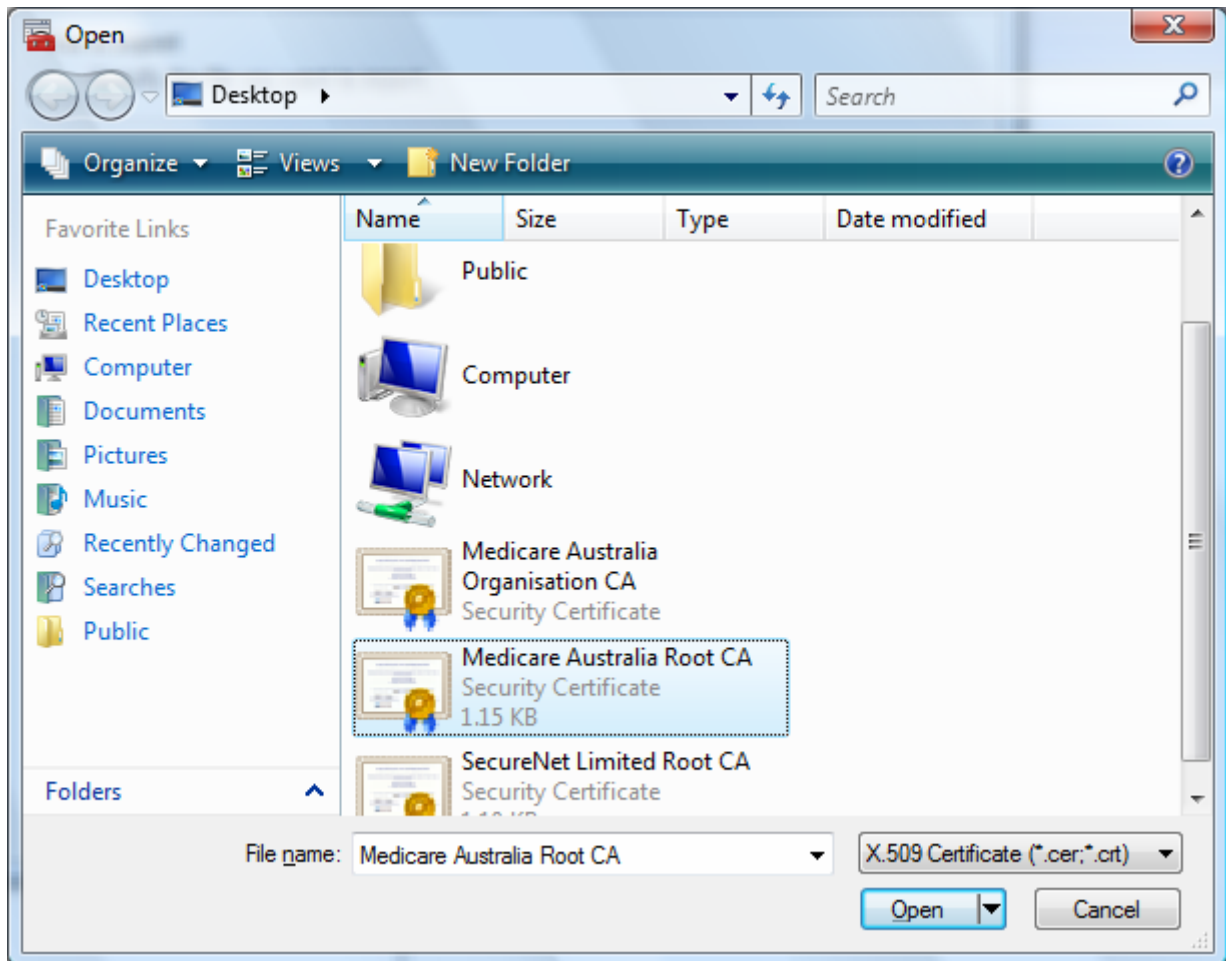


Figure 30: Medicare Australia Root CA location

Select the *Medicare Australia Root CA* and then click *Open*.

This will return you to the wizard at *Figure 29* above.

To continue click *Next*.

Step 27

The following screen will display.

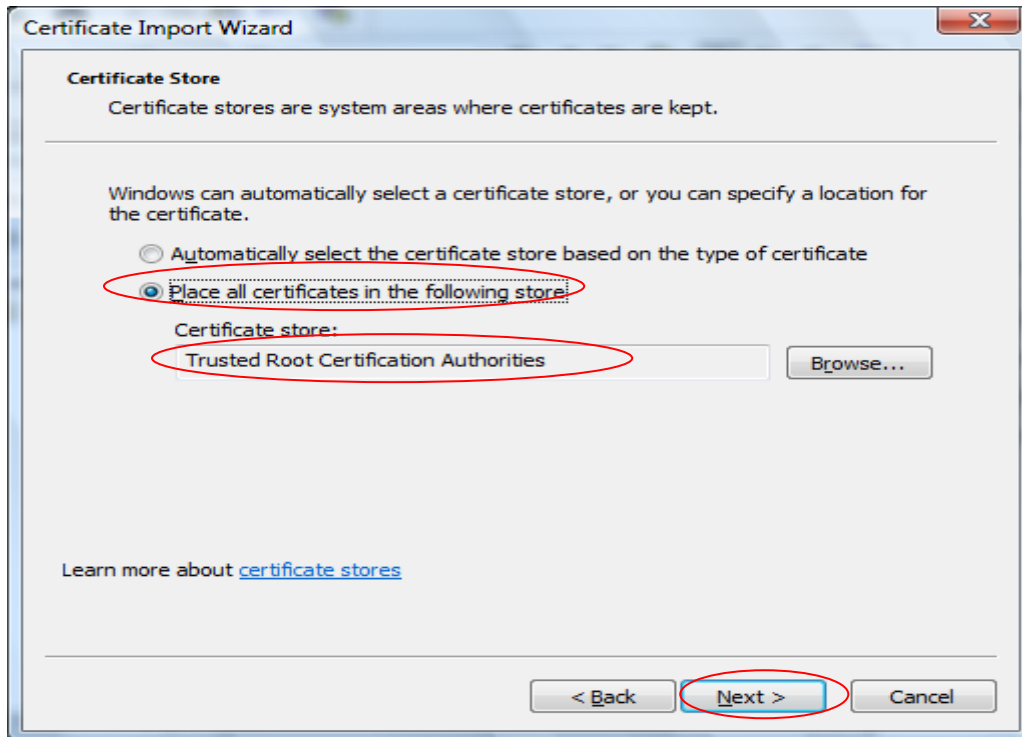


Figure 29: Certificate store

Select *Place all certificates in the following store Certification Authorities*.

The settings shown in *Figure 29* should automatically default for you if you have followed the previous steps.

To continue click *Next*.

Step 28

The following screen will display.

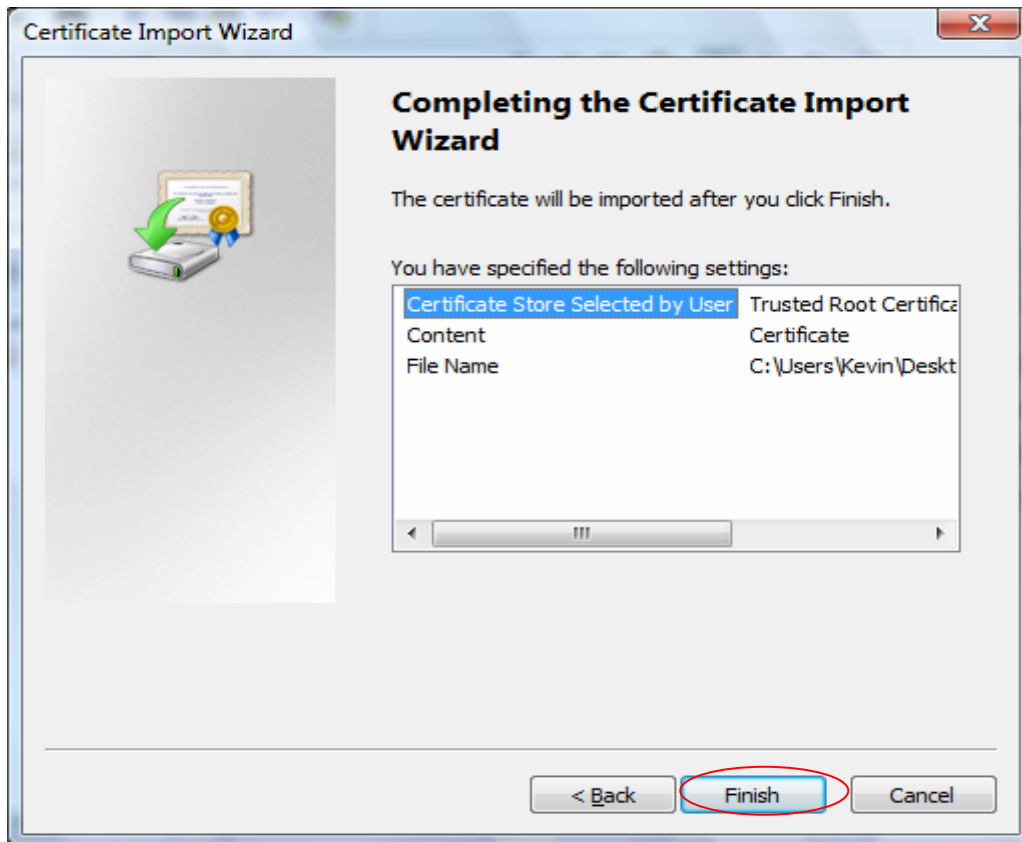


Figure 30: Finish screen

To continue click *Finish*.

The following message will appear.

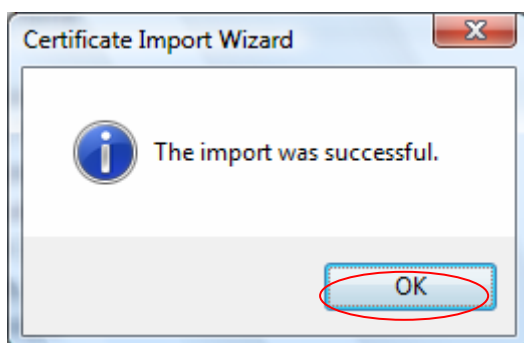


Figure 31: Successful install

Click *OK* to complete the Import Process.

Step 29

Repeat steps 24 - 28 for the *Intermediate Certification Authority Certificate* as shown in the following screenshot.

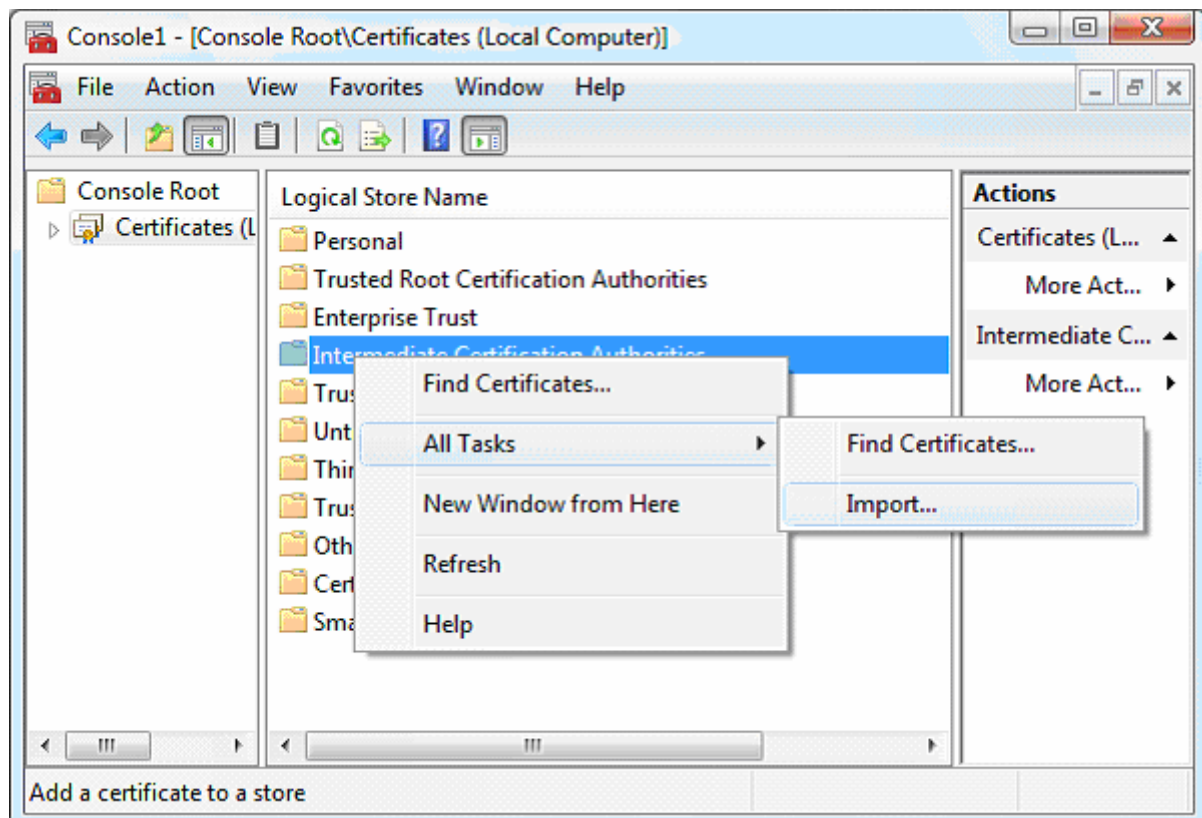


Figure 32: Intermediate Certificate Authority

You can now close the 'Console1' window.

You will be prompted to save Console1. If you choose to save it, it is recommended this is saved on the desktop and called 'Certificate Store'. In the future if there is a requirement to update the Microsoft Crypto Store with Medicare Australia chain of trust, you can simply double click on the appropriately named file on the Desktop.

You have successfully completed installing all components of the location certificate.

Important: Each computer that needs to access the HPOS page will need the certificate installed on that local machine.

If you continue to experience problems you can refer to our *Trouble Shooting Guide* or contact our eBusiness service centre on **1800 700 199**** for further assistance.

** Call charges apply from mobile and pay phones only.